Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for providing access management through use of a plurality of server machines associated with different locations, said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location;

authenticating a user of the first client machine;

authenticating the first client machine;

retrieving at the first server machine, based on the success of said authenticating of the user and authenticating of the first client machine, a user key permitting access to an individually encrypted sub-header of the secured item, the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other users or groups and comprising access rules applicable to the other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier;

permitting access to the secure item via the first location based on success of said authenticating of the user and authenticating of the first client machine, and further based on allowability by the access rules; and

permitting access to the secure item via the first server machine based on said permitting access to the secure system via the first location permitting the user to gain access to the secure item from the first location.

2. (Previously Presented) The method as recited in claim 1, wherein said permitting access to the secure system via the first location comprises:

obtaining access privileges associated with the user to determine at least one or more permitted locations for the user; and

determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user.

3. (Previously Presented) The method as recited in claim 1, wherein permission by said permitting access to the secure system via the first location further comprises allowing access to the secure item from the first location via the first client machine and the first server machine.

4. (Previously Presented) The method as recited in claim 1, wherein permission by said permitting access to the secure item via the first server machine further comprises allowing access to the secure item from the first location via the first client machine and the first server machine.

5. (Previously Presented) The method as recited in claim 1, further comprising:

preventing access to the secure item via any of the server machines other than the first server machine based on said permitting access to the secure item via the first server machine permitting the user to gain access to the secure item from the first location.

6. (Previously Presented) The method as recited in claim 1,

wherein said permitting access to the secure system via the first location comprises determining whether the user is permitted to gain access to the secure item via the first client machine and the first server machine, and

wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first client machine and the first server machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item via both the first client machine and the first server machine.

7. (Previously Presented) The method as recited in claim 1,

wherein said permitting access to the secure system via the first location comprises determining whether the user is permitted to gain access to the secure item via the first server machine, and

wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first server machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item via the first server machine.

8. (Previously Presented) The method as recited in claim 1,

wherein said permitting access to the secure system via the first location comprises determining whether the user is permitted to gain access to the secure item via the first client machine, and

wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first client machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item via the first client machine.

9. (Previously Presented) The method as recited in claim 1, further comprising:

preventing the user from gaining access to the secure item via any of the server machines other than the first server machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item from the first location.

10. (Previously Presented) The method as recited in claim 9, wherein said preventing the user from gaining access to the secure item via any of the server machines other than the first server machine comprises reconfiguring at least one of the server machines that previously permitted the user to gain access to the secure item therethrough.

11. (Previously Presented) The method as recited in claim 10, wherein said permitting access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine.

12. (Previously Presented) The method as recited in claim 11, wherein said permitting access to the secure system via the first location comprises:

obtaining access privileges associated with the user to determine at least one or more permitted locations for the user; and

determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user.

13. (Previously Presented) The method as recited in claim 1, wherein said permitting access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine.

14. (Previously Presented) The method as recited in claim 1, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file, the secured file having a format that comprises a header including security information as to who and how access to the secure item is permitted; an encrypted data portion including data of the secured file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

15. (Previously Presented) The method as recited in claim 14, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

16. (Previously Presented) The method as recited in claim 15, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information in the header of the secured file points to or includes the access rules and a file key.

17. (Previously Presented) The method as recited in claim 14, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information is encrypted with a user key associated with the user.

18. (Previously Presented) The method as recited in claim 14, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information includes the file key and access rules to the restricted access to the secured file.

19. (Previously Presented) The method as recited in claim 18, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file based on access privilege of the user being within access permissions by the access rules.

20. (Previously Presented) The method as recited in claim 18, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the access rules are expressed in a markup language.

21. (Currently Amended) A method for providing access management through use of a distributed network of server machines, said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine;

authenticating a user of the client machine;

authenticating the first client machine;

upon successfully authenticating the user and authenticating the first client machine, retrieving at the first server machine a user key permitting access to an individually encrypted sub-header of the secure item, the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secure item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other users or groups and comprising access rules applicable to the other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier;

retrieving access privileges associated with the user;

determining whether the user is permitted to gain access to the secure item via the first server machine based on success of said authenticating the user and said authenticating the first client machine, and further based on allowability by the access privileges and access rules; and

permitting access to the secure item via the first server machine based on said determining whether the user is permitted to gain access to the secure item via the first server machine determining that the user is permitted to gain access to the secure item via the first server machine.

22. (Previously Presented) The method as recited in claim 21, further comprising:

preventing access to the secure item via any of the server machines other than the first server machine based on said determining whether the user is permitted to gain access to the secure item via the first server machine determining that the user is permitted to gain access to the secure item via the first server machine.

23. (Previously Presented) The method as recited in claim 21,

wherein said determining whether the user is permitted to gain access to the secure item via the first server machine further determines whether the user is permitted to gain access to the secure item via the first client machine, and

wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first client machine and the first server machine based on said determining whether the user is permitted to gain access to the secure item via the first server machine determining that the user is permitted to gain access to the secure item via both the first client machine and the first server machine.

24. (Previously Presented) The method as recited in claim 23, further comprising:

preventing access to the secure item via any of the server machines other than the first server machine based on said determining whether the user is permitted to gain

access to the secure item via the first server machine determining that the user is permitted to gain access to the secure item via the first server machine.

25. (Previously Presented) The method as recited in claim 24, wherein said preventing access to the secure item via any of the server machines other than the first server machine comprises reconfiguring at least one of the server machines that previously permitted the user to gain access to secure items therethrough.

26. (Previously Presented) The method as recited in claim 25, wherein said permitting access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine.

27. (Previously Presented) The method as recited in claim 21, wherein said permitting access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access to the secure item via the first server machine.

28. (Previously Presented) The method as recited in claim 21, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file, the secured file having a format that comprises a header including security information as to who and how access to the secured file is permitted; an encrypted data portion including data of the secured file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

29. (Previously Presented) The method as recited in claim 28, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

30. (Previously Presented) The method as recited in claim 28, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information is encrypted with a user key associated with the user.

31. (Previously Presented) The method as recited in claim 28, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the security information includes the file key and access rules to the restricted access to the secured file.

32. (Previously Presented) The method as recited in claim 28, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file based on access privilege of the user being within access permissions by the access rules.

33. (Previously Presented) The method as recited in claim 31, wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file wherein the access rules are expressed in a markup language.

34. (Currently Amended) A ~~tangible~~ computer-readable ~~medium~~ storage device having computer-executable instructions stored thereon to cause a computing device to perform a method for providing access management to secured content through use of a plurality of server machines associated with different locations, the method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location;

authenticating a user of the first client machine;

authenticating the first client machine;

retrieving at the first server machine, based on the success of said authenticating of the user and authenticating of the first client machine, a user key permitting access to an individually encrypted sub-header of the secured item, the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secure item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other users or groups and comprising access rules applicable to the other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier;

determining whether access to the secure item via the first location is permitted based on success of said authenticating the first client machine and the user, and further based on allowability by the access rules;

permitting access to the secure item via the first server machine based on said determining that the user is permitted to gain access to the secure item from the first location; and

preventing access to the secure item via the first server machine based on said determining that the user is not permitted to gain access to the secure item from the first location.

35. (Currently Amended) A ~~tangible~~ computer-readable ~~medium~~ storage device having instructions stored thereon for providing access management through use of a distributed network of server machines, the instructions comprising:

instructions to receive, at first server machine of the plurality of server machines, an access request to access a secure item from a first client machine;

instructions to authenticate a user of the client machine;

instructions to authenticate the first client machine;

instructions to retrieve at the first server machine, based on the success of said authenticating of the user and authenticating of the first client machine, a user key permitting access to an individually encrypted sub-header of the secured item, the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secure item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other users or groups and comprising access rules applicable to the other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on ~~an~~ a corresponding user or group identifier;

instructions to retrieve access privileges associated with the user;

instructions for determining whether the access to the secure item via the first server machine is permitted based on success of said instructions for authenticating the

first client machine and the user, and further based on allowability by the access privileges and access rules;

instructions to permit access to the secure item via the first server machine based on said computer program code for determining making a determination that the user is permitted to gain access to the secure item via the first server machine; and

instructions to prevent access to the secure item via the first server machine based on said computer program code for determining making a determination that the user is not permitted to gain access to the secure item via the first server machine.

36. (Currently Amended) An access control system that restricts access to a secure item, said system comprising:

a central server having a server module that provides overall access control; and

a plurality of local servers, each of said servers including a local module that provides local access control,

wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors,

wherein, based on information stored in an individually encrypted sub-header of a secure item, a given requestor is permitted to access the secure item through one or more of said local servers, the information stored in the individually encrypted sub-header of the secure item comprising access rules applicable to the requestor or to a group to which the requestor belongs, and

wherein the individually encrypted sub-header is selected for decryption by the given requestor from a group of one or more additional individually encrypted sub-headers corresponding to other requestors or groups to which the other requestors belong

and comprising access rules applicable to the other users or groups, based on correspondence of the individually encrypted sub-header to a corresponding user or group identifier for the given requestor or to the group to which the requestor belongs.

37. (Previously Presented) The access control system as recited in claim 36, wherein said access control system couples to an enterprise network to restrict access to the secure item, which comprises a secured file, stored therein.

38. (Previously Presented) The access control system as recited in claim 37, wherein the access requests are at least primarily processed in a distributed manner by said local servers.

39. (Previously Presented) The access control system as recited in claim 38, wherein the requestors gain access to the secured files without having to access said central server based on processing of the access requests by said local servers.

40. (Previously Presented) The access control system as recited in claim 37, wherein the local module is a copy of the server module so any of the local modules operate independently of said central server and other of said local servers.

41. (Previously Presented) The access control system as recited in claim 37, wherein the local module is a subset of the server module.

42. (Previously Presented) The access control system as recited in claim 37, wherein access permissions for said local servers is dynamically configured to pass a requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as a change of the location of the requestor.

43. (Previously Presented) The access control system as recited in claim 37, wherein the secured files are secured by encryption of the secure item.

44. (Previously Presented) The access control system as recited in claim 37, wherein the secure item is secured by encryption.

45. (Currently Amended) A method for providing access management through use of a plurality of server machines associated with different locations, said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location;

authenticating a user of the first client machine;

authenticating the first client machine;

retrieving at the first server machine, based on the success of said authenticating of the user and authenticating of the first client machine, a user key permitting access to an individually encrypted sub-header of the secured item, the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item, the sub-header selected, from a group of individually encrypted sub-

headers corresponding to other users or groups and comprising access rules applicable to the other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier;

permitting access to the secure item via the first location based on success of said authenticating of the user and authenticating of the first client machine, and further based on allowability by the access rules; and

preventing access to the secure item via the first server machine based on said permitting access to the secure system via the first location not permitting the user to gain access to the secure item from the first location.

46. (Currently Amended) A method for providing access management through use of a distributed network of server machines, said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine;

authenticating a user of the client machine;

authenticating the first client machine;

upon successfully authenticating the user and authenticating the first client machine, retrieving at the first server machine a user key permitting access to an individually encrypted sub-header of the secure item, the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secure item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other users or groups and comprising access rules applicable to the other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier;

retrieving access privileges associated with the user;

determining whether the user is permitted to gain access to the secure item via the first server machine based on success of said authenticating the user and said authenticating the first client machine, and further based on allowability by the access privileges and access rules; and

preventing access to the secure item via the first server machine based on said determining whether the user is permitted to gain access to the secure item via the first server machine determining that the user is not permitted to gain access to the secure item via the first server machine.